Leitfaden für GDPR

Update v1.1 | April 2019

Anmerkung der Redaktion: Dieses Dokument wurde von Alan Robinson für AAMET zusammengestellt.

Was ist Datenschutz?

RECHTLICHE REGELN, die gelten, wenn wir Daten einer identifizierbaren Person verarbeiten.

Was ist GDPR?

Es ist die **Allgemeine Datenschutzverordnung**.

- Größte Überarbeitung des Datenschutzes seit dem Data Protection Act 1998.
- Es ist eine EU-Verordnung und gilt mit direkter Wirkung für alle EU-Mitgliedstaaten.
- Sie ändert die bestehenden Vorschriften für den Umgang mit Daten, um Transparenz und Rechenschaftspflicht zu erhöhen.
- Es wird IRRESPECTIVE OF BREXIT anwenden.

Warum betrifft es Freiwilligenorganisationen?

Die Datenschutzgesetzgebung gilt für alle für die Datenverarbeitung Verantwortlichen.

Ein Datenverantwortlicher ist

- Eine natürliche oder juristische Person, Behörde, Agentur oder andere Stelle.....
- Wer oder was allein oder gemeinsam mit anderen....
- Legt die Zwecke und Mittel der Verarbeitung personenbezogener Daten fest.

Das bedeutet, dass....

- JEDE Organisation oder Gruppe....
- der jede Art von personenbezogenen Daten enthält, UND....
- ist verantwortlich für die Entscheidung, was mit diesen Informationen passiert....

.... ist ein Datenverantwortlicher.

Sie müssen zeigen, dass Sie die Risiken bei der Verarbeitung von Daten anderer Personen verstehen. Das bedeutet, grundlegende Informationen zu haben, um dies zu darlegen.

Was sind personenbezogene Daten?

Sie gilt für alle personenbezogenen Daten über lebende Personen.

Es identifiziert eine Person:

- Susan Smith wahrscheinlich nicht.
- Alan Robinson möglich, insbesondere wenn z.B. mit einer E-Mail-Adresse verlinkt.
- Sir Andy Murray definitiv

Es umfasst alle Personen - Mitarbeiter, Freiwillige, Kunden oder Kunden, Begünstigte, Sie...

Es gilt, was immer Sie mit den Daten machen - sammeln, verwenden, löschen, anonymisieren und alles dazwischen.

Einige Daten sind **sensible persönliche Daten**.

Dazu gehören:-

- Rassische/ethnische Herkunft,
- Politische Meinungen,
- Religiöse oder philosophische Überzeugungen,
- TU-Mitgliedschaft,
- Genetisch/biometrisch zur Identifizierung,
- Gesundheit,
- Sexualleben und sexuelle Orientierung.

Generell ist für die Verarbeitung sensibler Daten AUSDRÜCKLICHE ZUSTIMMUNG erforderlich. Es genügt, wenn die betroffene Person sie öffentlich zugänglich gemacht hat.

Wie können wir personenbezogene Daten verarbeiten?

DAS ERSTE PRINZIP DER DATENVERARBEITUNG
DIE VERARBEITUNGSDATEN MÜSSEN FAIR, TRANSPARENT UND RECHTMÄßIG SEIN.

Um rechtmäßig zu sein, muss sie eine Bedingung in Artikel 6 erfüllen.

Artikel 6 Bedingungen

- **Zustimmung**, die klar, nachweisbar, freiwillig erteilt, leicht entziehbar und unmissverständlich ist.
- Daten, die für die **Zwecke eines Vertrages** verarbeitet werden.
- Es besteht eine **gesetzliche Verpflichtung** zur Aufbewahrung der Daten.
- Die Verarbeitung der Daten liegt im **vitalen Interesse** einer Person (sicherer, sich nicht darauf zu verlassen).

- Die Verarbeitung der Daten ist im **öffentlichen Interesse** erforderlich (sicherer, sich nicht darauf zu verlassen).
- Die Verarbeitung der Daten ist für die **legitimen Interessen des Unternehmens** notwendig, und die Interessen des Einzelnen werden dadurch nicht beeinträchtigt.

Im Allgemeinen erwarten wir die Zustimmung der betroffenen Person. Können Sie die Definition von Zustimmung erfüllen? Das Subjekt muss sich ein- und nicht austragen. Die Zustimmung im alten Stil ist vielleicht nicht genug.

FAIRE VERARBEITUNG - EIN BEISPIEL
Das Gemeindezentrum möchte ein Foto und den Namen eines Kindes, das an einer kürzlich stattgefundenen Veranstaltung teilgenommen hat, in seinem Gemeinde-Newsletter verwenden.

GILT DAS ERSTE DATENSCHUTZPRINZIP.

Die Verarbeitung muss erfolgen:
- FAIR
- TRANSPARENT
- GESETZLICH

Ist das fair?

Schauen Sie sich die Umstände an, unter denen Sie die Informationen erhalten haben.

- Es war eine öffentliche Veranstaltung.
- War es klar, warum du die Fotos gemacht hast? Professioneller Fotograf oder "snap"?

Was wäre unter diesen Umständen ein sinnvoller Nutzen?

Welcher Zusammenhang besteht zwischen der Verwendung, für die Sie die Informationen gesammelt haben, und der Verwendung, für die Sie sie verwenden möchten?

Ist es transparent?

- Wie offensichtlich ist dieser Nutzen?
- Was haben Sie Ihren Besuchern und Nutzern darüber gesagt, was Sie mit ihren Informationen machen wollen?
- Was steht in Ihrer Datenschutzerklärung?
- Was steht in Ihrem ICO-Registereintrag (falls vorhanden)?

Ist es rechtmäßig?

Können Sie eine Bedingung in Artikel 6 erfüllen?

- Hast du die Zustimmung des Kindes dazu? Wie alt ist das Kind? Was ist mit den Eltern? Kannst du beides dazu bringen, dich zu schützten?
- Oder ist es notwendig, dass eine Aufgabe im öffentlichen Interesse ausgeführt wird?
- Oder notwendig für die legitimen Interessen des Zentrums? Was ist mit Vorurteilen gegenüber den Individuen? Wenn du ein Foto vom Sommerspaßtag im Frauenhaus machst und es an die Presse schickst, kann es zu schweren Beeinträchtigungen der Interessen der Betroffenen kommen.
- Wird sie Informationen über das Kind öffentlich machen? Wenn das Zentrum zum Beispiel glaubwürdig ist, macht es dann öffentliche Informationen über die Religion des Kindes?
- Wenn ja, gibt es eine ausdrückliche Zustimmung? Oder sind die Informationen bereits öffentlich zugänglich?

Was ist neu an GDPR?

Anforderung an bestimmte Richtlinien

- Datenschutzhinweise
- Datenschutzfolgenabschätzungen - neue Anforderung an die risikoreiche Verarbeitung
- Datenverarbeitungsvereinbarungen - neue Anforderungen
- Individuelle Rechte (Recht auf Vergessen, Portabilität etc.)

Der Nachweis ist der Schlüssel. Kannst du beweisen, dass du alles getan hast, was du tun musst?

Was müssen Sie jetzt tun?

- Führen Sie ein Datenaudit durch. Welche Daten speichern Sie und warum?
- Überprüfen Sie die von Ihnen gespeicherten Daten und prüfen Sie, ob Sie das erste Prinzip einhalten.
- Erstellen Sie Datenschutzhinweise und stellen Sie diese allen Personen zur Verfügung, deren Daten Sie speichern.
- Brauchst du ihre Zustimmung? Wenn ja, stellen Sie sicher, dass Sie es schriftlich haben. Wenn Sie dies nicht tun, müssen Sie entweder die Daten löschen oder entscheiden, welche andere Bedingung von Artikel 6 anwendbar ist - und diese aufzeichnen.
- Stellen Sie sicher, dass Sie über alle relevanten Richtlinien verfügen.
- Wenn Sie über Datenverarbeitungsverträge verfügen, überprüfen und ändern Sie diese.
- Stellen Sie sicher, dass Sie über ein Verfahren verfügen, bei dem Personen ihre individuellen Rechte ausüben können.
- Stellen Sie sicher, dass alle Ihre Mitarbeiter, Freiwilligen usw. wissen, was sich geändert hat. Schulen Sie Ihre Mitarbeiter. Stellen Sie sicher, dass Sie nachweisen können, dass Sie dies getan haben.

Datenschutzhinweise

Wenn Sie Daten erheben, müssen Sie den Personen, die die Daten zur Verfügung stellen, einen **DATENSCHUTZVERMERK** geben. Dazu gehören:

- Die Identität und Kontaktdaten der verantwortlichen Stelle und jedes Datenverarbeiters (siehe unten);
- Die Zwecke, für die Informationen gesammelt werden;

- Die Rechtsgrundlage für die Nutzung von Informationen:
    - Wenn Zustimmung - erwähnen Sie, dass sie die Zustimmung widerrufen können;
    - Wenn es für berechtigte Interessen notwendig ist - geben Sie an, welche Interessen dies sind;
    - Wenn gesetzliche Anforderung oder Vertrag - ob obligatorisch oder nicht obligatorisch und die Folgen der Nichterfüllung.
- Empfänger/Kategorien von Empfängern;
- Einzelheiten zu den Sicherheitsvorkehrungen außerhalb der europäischen EA;
- Aufbewahrungsfrist oder Kriterien zur Bestimmung der Dauer;
- Das Bestehen des Rechts auf Zugang zu Informationen, Berichtigung, Löschung, Widerspruch gegen die Verarbeitung und Datenübertragbarkeit;
- Das Recht, sich beim ICO zu beschweren.

Richtlinien

DU MUSST Policen haben, die Folgendes abdecken....

- Was passiert, wenn es einen Datenverstoß gibt? Muss dem ICO innerhalb von 72 Stunden mitgeteilt werden, es sei denn, es handelt sich um einen Verstoß gegen die Vorschriften. Muss nicht an Einzelpersonen weitergegeben werden (aber eine gute Idee).
- Datenspeicherung - wie lange werden die Daten gespeichert?
- Verwendung sensibler Informationen für die Beschäftigung
- Verwendung von DBS-Informationen. Das ist es, was wir haben; das ist es, wie wir es sicher aufbewahren.

Eine allgemeine Datenschutzerklärung ist optional, kann aber alle notwendigen Informationen enthalten, um die Anforderungen der Richtlinie zu erfüllen.

Möglicherweise benötigen Sie eine BYOD-Richtlinie (bringen Sie Ihr eigenes Gerät mit). Ob Sie eine Richtlinie haben oder nicht, SIE MÜSSEN ANMERKEN, WANN DIESE ANWENDUNGEN - das Problem der Mitarbeiter und Freiwilligen, die Daten auf ihren eigenen Computern oder Telefonen verarbeiten.

Datenverarbeiter

Ein Dritter, der unter Ihrer Anweisung und Kontrolle handelt, wenn er für Sie etwas mit personenbezogenen Daten macht - zum Beispiel Lohnbuchhalter.

Sie sollten bereits eine schriftliche Vereinbarung haben, aber es gibt jetzt zusätzliche Anforderungen.

Überprüfen Sie insbesondere IT-Verträge

Hinzufügen:

- Vertraulichkeitsverpflichtung des Personals;
- Unterauftrag mit Erlaubnis des Controllers;
- Unterstützung des Controllers bei den Themenrechten und der Sicherheit;
- Zurückkehren oder Löschen am Ende - nach Wahl des Controllers;
- Stellen Sie dem Controller Informationen über die Aktivität zur Verfügung.

Individuelle Rechte

- Themenzugang - 30 Tage - kostenlos
- Berichtigung - Recht auf Berichtigung der Daten.
- Löschung - Recht auf Vergessenheit
- Einschränkung - Recht, die Verwendung von Daten auf die Speicherung zu beschränken, aber nicht zu verarbeiten.
- Portabilität - Speichern und Verwenden personenbezogener Daten für eigene Zwecke in einer Reihe von Einstellungen.

Daten-Audits

Der erste Schritt ist die **Durchführung eines Datenaudits**. Auf diese Weise werden Sie mit ziemlicher Sicherheit sehen können, welche Daten Sie sammeln und wofür, und was Sie dagegen tun müssen.

Was Sie wissen müssen:

- Welche Daten Sie haben,
- Wo es ist,
- Warum du es hast,
- Wie du es bekommen hast,
- Was man damit macht,
- Wie lange du es brauchst.

Daten-Audit: Was

Erinnern Sie sich an die Definition von personenbezogenen Daten.

Identifizieren Sie, welche Kategorien Sie als Unternehmen haben.

- Mitarbeiter/Freiwillige
- Mitglieder der Organisation
- Reguläre Spender
- Auftragnehmer
- Gibt es noch mehr?

Welche Informationen haben Sie über jede Kategorie?

Daten-Audit: Wo

Wo speichern Sie Ihre Daten?

PAPIER

- Aktenschränke

- Heimbüro
- Schubladen
- Servietten.... ist diese Telefonnummer auf dem Post It auf dem Brett persönliche Daten? Das könnte es sein!

ELEKTRONISCH

- Datenbanken
- Personal Computer
- Speichersticks
- CDs
- Telefone oder Laptops von Mitarbeitern oder Freiwilligen?
- Disketten????

Daten-Audit: Warum?

Warum hältst du die Daten, die du machst?

Das hängt davon ab, was es ist.

- Persönliche Kontaktdaten für Kunden
- Kommunikation über Ereignisse
- Sitzungseinladungen
- Informationen zur Lohn- und Gehaltsabrechnung
- Mitarbeiterinformationen
- Disziplinarische Aufzeichnungen
- Gebetsanliegen an eine Gemeinde
- Kontaktdaten der Kuratoren und Ausschussmitglieder
- Taufregister für eine Kirche
- Was noch?

Daten-Audit: Wie werden Daten erhoben?

Von der Person
Von einer anderen Person

- Freund
- Relativ
- Statutarische Stelle/Organisation
- Frühere Berater
- Vorherige Kirche
- Soziale Medien.....

Daten-Audit: Was machst du mit den Daten?

Nochmals - hängt von den Informationen ab.

- Wofür benutzt du es?
- Wofür willst du es verwenden?
- Wofür solltest du es verwenden?

- Übertragen Sie es an Dritte?
    - Regelmäßig
    - Als Einzelstück, gelegentlich.
- Gibt es "Transfers" von elektronischem Material auf Server außerhalb des Standorts? Wie werden diese Daten geschützt? Sie sollten sich z.B. von Googledocs informieren lassen.
- Benutzt du die Cloud? Wie wird das geschützt?

Daten-Audit: Wie lange benötigen Sie die Daten?

Gibt es gesetzliche Anforderungen, wie z.B. eine Mindestzeit zur Aufbewahrung?

Wenn nicht.....

- - Wie lange willst du es haben?
- - Können Sie diese Zeitspanne rechtfertigen?

Wenn ja - so lange kannst du es behalten!

Daten-Audit: Wenden Sie die Grundsätze auf Ihre Daten an.

Erinnere dich an das erste Prinzip: Die Verarbeitung muss fair, transparent und rechtmäßig sein.

Was ist sinnvoll? (FAIR)

Was hast du ihnen gesagt, als du ihre Informationen erhalten hast? (TRANSPARENT)

Können Sie eine Bedingung für Artikel 6 erfüllen? (GESETZLICH)

Artikel 6 Bedingungen

- Klar, nachweisbar, freiwillig, spezifisch für jeden Zweck erforderlich, leicht entziehbar, eindeutige Einwilligung
- Vertragszwecke
- Rechtliche Verpflichtung
- Wichtige Interessen (z.B. Details zur nächsten Verwandtschaft)
- Öffentliches Interesse
- Notwendig für berechtigte Interessen ohne Beeinträchtigung.

Und vergiss nicht....

- Verwenden Sie die Daten nur für den Zweck, für den sie erhoben wurden.
- Nur das haben, was Sie brauchen
- Halten Sie alles genau und auf dem neuesten Stand.
- Bewahren Sie es nur so lange auf, wie Sie es benötigen.
- Bewahren Sie die Daten sicher auf. Du entscheidest, was sicher ist. Es ist notwendig, das Risiko zu bewerten und nachzuweisen, dass dies geschehen ist.
- Sicherstellen, dass Einzelpersonen auf ihre Rechte zugreifen können.

- Transportieren Sie nicht ohne Zustimmung oder Schutzmaßnahmen außerhalb des Europäischen Wirtschaftsraums.

Beispiel für eine Audit-Tabelle für eine Freiwilligenorganisation:

WER	WAS	FAIR	TRANSPARENT	BEDINGUNG
Treuhänder	Bank Details Persönliche Adressen E-Mail Adressen	ja	Siehe Datenschutz-erklärung	Einwilligung Notwendig für ein berechtigtes Interesse
Personal	Familienstand / sexuelle Orientierung1	ja	Siehe Datenschutz-erklärung	Gesetzliche Anforderungen? Einwilligung? Legitime Interessen? ???
Benutzer	Foto beim Kirchenfest2	vielleicht	Vielleicht. Frühere Beispiele?	Einwilligung? Legitime Interessen?
Freiwillige	Privatadressen Telefonnummern E-Mail-Adressen	ja	Siehe Datenschutz-erklärung	Einwilligung Legitime Interessen

[1] – kann unvermeidlich sein, z.B. wenn der Mitarbeiter den Titel oder den Namen der nächsten Angehörigen verwendet.
[2] – siehe Beispiel oben

Deutsche Übersetzungen 16.07.2019